2011 UKSim 13th International Conference on Modelling and Simulation

A Conceptual Design of Novel Modern Random Key-Stream Generator for High Immunity Correlation Attack

Ashwak M. AL-Abiachi
Information Technology Department
University Utara Malaysia
ashwakalabaichi2007@yahoo.com

Faudziah Ahmad
Information Technology Department
University Utara Malaysia
fudz@uum.edu.my

Ku Ruhana
Information Technology Department
University Utara Malaysia
ruhana@uum.edu.my

***Abstract*—recently, the rapid development and the common use of electronic data processing administered through the Cyberspace, cooperatively with many incidents of attacks and breaches, fuelled the need for better methods of defending the computers and the information they store, process, and transmit. According to these difficulties, this research seeks to design a novel modern key-stream generator for high immunity correlation attacks. The research stated the main components of the proposed method, which divided into three diminutions RMA, MFSR & VLFCSR, and PER with 32 number to diffuse the output.**

Keywords: Key-stream, crypto, network security, network threats

I. INTRODUCTION

The development of security methods over the network has reflected the way of designing and coding these methods. However, the data security recognized as an issue that involves unlimited perspective towards securing data from the unknown threats [1]. The utilization of unsecured channels for communication has launches the process for determining an alternative solution towards the strength of security methods against attackers. For that reason, current attempts addressed the requirements for developing a new method and protocols in order to provide secure communication over public and unsecured communication channels [2].

Besides, securing data and information can be impeded through functioning of several techniques such as; encryption that reports as a best recognized technique, which includes a securing method to secure information from being read by unauthorized side [3]. Meanwhile, encryption also helps to convert the plaintext to a cryptic text in terms of securing data from other users. The conceptual process of cryptic text depends on the decrypted with the other termination to be declared and acknowledged over the network. This process requires the adopting of systematic or a certain step called an algorithm to convert the text contents to the initial message, known as plaintext, into cipher text [4]. Moreover, the process of cryptographic algorithms commonly needs sequences of organized variables known as a key to encrypt or decrypt the contents of data. The converting process from plaintext into cipher text is requiring a certain key for identifying the text characters to be decrypted again into plaintext [5].

There are several dimensions that cryptographic are depending on it during the securing process of the data over the network:

Based on the form of the encrypting operations, there are two common methods that employed for converting plaintext to a cipher text such as; substitution and transposition. On the one hand, substitution deals with each element in the plaintext (bit, letter, group of bits or letters) being followed with another element. On the other hand, transposition is dealing with the elements in the plaintext within a re-arrangable form [6].

Based on the numbers of keys in the structure. An example, when the crypto process among the sender and receiver within the same key, the system will be directed to as symmetrical, single-key, secret-key, or conventional encryption. As well as the use of alternative keys will be directed as unsymmetrical, two-key, or public encryption.

Based on the plaintext process, the process of the block cipher to be conducted one block of elements, which causes to the construction of an output block. In comparison, the stream cipher processes the input elements continuously, producing one output element at a time, as it continues.

II. ISSUES

Stream ciphering appears to be one of the best options in order to set confidentiality to high-speed communications. To ensure the security effectiveness of the stream ciphers a number of comprehensions have been recommended in order by other researchers. The most important issue is the linear complexity of the key-stream, randomness, and correlation immunity attacks. On the other hand, linear feedback shift register (LFSR) known as a shift register, which demonstrates as a linear function of its previous state.

Correlation attacks are occurs usually between the individual LFSE and the Boolean in the key-stream. These attacks initialled when there is a consequential association among the output of LFSR and the output of Boolean function, which merges the output state of all the LFSRs in the correlation [6]. This process involves the combination of the partial knowledge of the key-stream for permitting an attacker to brute-force the key for that LFSR and the rest of the system individually. Example of that process, when the four 8-bit LFSRs are represented into the key-stream generator to carry out the key-stream and one of the directories is correlate to the Boolean output. Hence, for determining the absolute attack complicatedness of 28 + 224. In this appreciation, correlation attacks can be represented to distribute and defeat algorithms [7]. Also, it directly determines security and efficiency, but most of the

978-0-7695-4376-5/11 $26.00 © 2011 IEEE
DOI 10.1109/UKSIM.2011.82

utilized key streams are binary valued, and suffer from short period and limited key space. Thus, providing a novel modern random key-stream generator for securing the contents of data in the high immunity correlation attack.

III. RELATED WORKS

According to Awad, proposed a new approach for finding the linear equivalence of key stream generators. The study presents two simulated annealing algorithms which have been applied to solve this problem. Both algorithms use genetic operations to modify the candidate solutions. The performance evaluation is carried out for a set of key stream generators and the results are compared with the results of applying genetic algorithm to solve the same problem. The proposed algorithms are able to find the linear equivalence and more effective than genetic algorithm [8].

A study by Faraoun described the recent dev elopement of cryptosystems based on chaos. Furthermore, Faraoun addressed the main difficulties in terms of low level of security and small key space. Thus, Faraoun developed an n-ary key stream generator, based on hierarchical combination of three chaotic maps. The study conducted that the propose key stream have a good statistical properties in term of uniform distribution, δ-like auto-correlation function, near-zero cross-correlation and very height sensitivity to initial conditions, under precision restricted condition. The obtained result indicated that n-ary key stream generator have enough secure to resist various attacks [9].

IV. METHOD

This study adopted the using of test driven approach by [10] which consist on coding and testing the proposed technique (a novel modern random key-stream generator). The proposed modern random key-stream generator called (ASH-32) consists of three major components that are: shift registers, RAM, and PER. The shift registers divided into multiplexer feedback shift register (MFSR) as shown below and VLFCSR. RAM consists of eight RAM with 256 x 256 one for each SR. Four multiplexer feedbacks 16x16 for MFSR set. PER is permutation with 1 x32 bits which the output of key generator comes out from it.

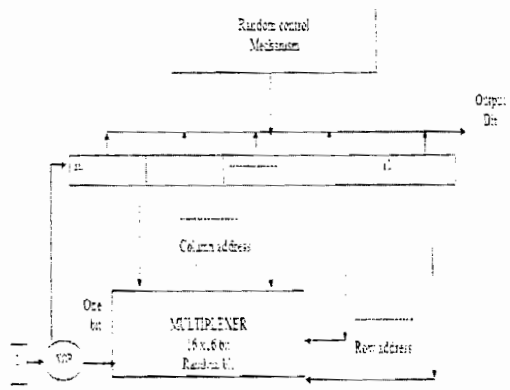


Figure 1. The proposed Multiplexer Feedback Shift Register (MFSR)

Meanwhile, the variable lengths of feedback with carry shift register (VLFCSR) are extension of the principle of traditional FCSR as shown in the figure below:

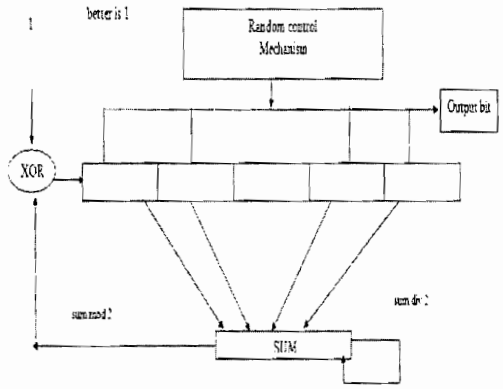


Figure 2. VLFCSR Structure

V. DEVELOPMENT AND RESULT

The proposed key generator (ASH-32) classifies into three dimensions:

- Shift registers
- RAM
- PER

Shift register contains two sets of shift registers; the first set consist of four shift registers of type MFSR of length (128,127,123,121) and the second set consist of four shift register of type FCSR with change shift register to be variable length.

The second part is RAM where consists eight RAM's work as S-boxes, each RAM used to determine the stage of each shift register where contain of it become the output of shift register then shifting contain of RAM circularly.

Finally, the PER presents a permutation table 1 x 32 used to permutation the output of shift register-set as illustrated in Figure 3 below:

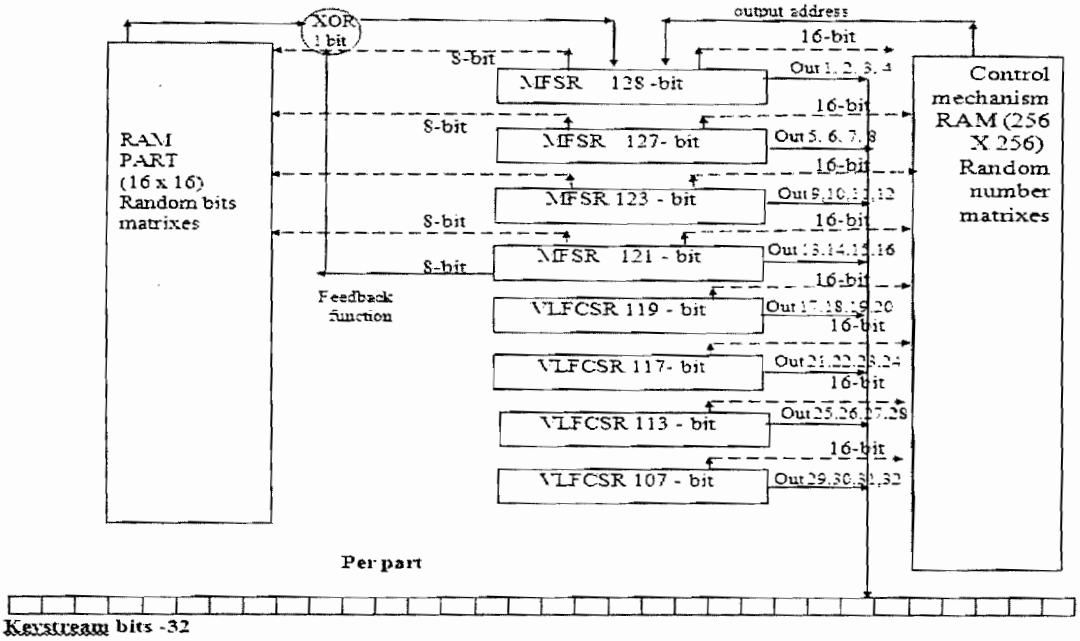


Figure 3. The proposed random key-generator process

After the initialization process is completed the following steps of generator ASH-32 will be initialled:

- 16 bits will be extracted from fixed stages in each shift register in shift register-part to use as addresses for RAM's in RAM-part.

RAM consists of eight RAM with 256 x 256 one for each SR with a random numbers that generated by special mechanism, the first RAM contain random number 0-127, the second 0-126 and so on based on the length of SR's

Moreover, the eight bits consists on (0... 255) by referring to the row address and the others eight bits (0...255) to the column address; theses stages that acts of row and column respectively for shift register.

Stages for row address (1)

({117, 19, 55, 70, 30, 12, 127, 90}, {1, 33, 88, 13, 24, 56, 77, 40}, {0, 3, 9, 10, 17, 37, 55, 23}, {11, 120, 15, 20, 22, 102, 111, 101}, 116, 25, 45, 78, 91, 42, 20, 19}, {66, 99, 88, 77, 55, 22, 33, 11}, {45, 47, 13, 22, 56, 50, 99, 17}, {104, 102, 101, 29, 23, 12, 30, 48}}

Stages for column address (2)

{{1, 13, 77, 120, 118, 125, 18, 7}, {70, 40, 23, 66, 79, 82, 34, 55}, {19, 119, 121, 117, 50, 80, 9, 109}, {120, 17, 5, 45, 77, 16, 35, 49},{101, 55, 68, 67, 23, 56, 90, 21}, {109, 105, 18, 77, 60, 42, 44, 12}, {105, 113, 22, 5, 45, 78, 89, 99}, {12, 34, 56, 89, 97, 52, 15, 66}}

- Convert each row's to decimal by multiply the following number (16, 1, 4, 8, 64, 128, 2, and 32).
- Intersection the row address with the obtained result of column addresses of each shift register where the output bit initialed successfully.
- Then 8 bits will be extracted from other fixed locations as a multiplexer address.
- After that, three bits will be extracted from each shift register based on the obtained result from the previous step to become 32 bits, in terms of the following equation:

Obj+1=obj +key * j mod L
j= 1...3,
L acts length of SR
Key acts secret key.

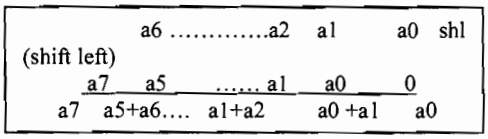
Four multiplexer feedbacks 16x16 for MFSR set are:

- The four bits represent (0..15) refers to the row address.
- Intersection the value of row address with obtained result from the column addresses bit X-ORed fixed is 1 result feedback bit.
- The modification process includes RAM, which presents the feedback function by shifting the contents circularly.

However, PER is permutation with 1 x32, which presents the output of key generator. PER perform the swapping process for two values in permutation table that

address these values based on the fixed stages of MFSR then shifting the values circularly. The initialization process starts by reading secret basic key16 character as seed key (or secret key) from the generator that is expanded to the 955 bits to fill all shift registers vertically, the following techniques is used in expansion key:

- Create coding table of 128 symbols of 7 bits for each see in appendix.
- The secret basic key is expanded into 8 bit as in the following:



VI. Expected Benefits

The developed random key-stream generator had obtained a high speed and security. This study expected to:

- Create a long period and linear complexity from the key-stream generator.
- Increase the randomization of key-stream generator by customizing the output of key-stream generator randomly.
- Creates a key-stream bit with high immunity correlation attack.
- Provides a novel modern random key-stream generator with 32 bit as output.

VII. Conclusion

Due to the difficulties in securing the information, which changed the ways for observing the key generator in terms of randomization, unpredictable, uniform distribution as well as large linear complexity immunity correlation attacks. The main goal of this study was to design a novel modern random key stream generator for high speed applications such as video, image, audio. The proposed random key-stream generator has been classified into three diminutions namely; RAM for determining the stage address of each shift register randomly, MFSR & VLFCSR, and PER with 32 number to diffuse the output.

References

[1] F. Armknecht, et al., "Efficient computation of algebraic immunity for algebraic and fast algebraic attacks," Advances in Cryptology-EUROCRYPT 2006, pp. 147-164, 2006.

[2] Y. Hu, et al., "A true random number generator based on mouse movement and chaotic cryptography," Chaos, Solitons & Fractals, vol. 40, pp. 2286-2293, 2009.

[3] I. Mantin, "Predicting and distinguishing attacks on RC4 keystream generator," Advances in Cryptology–Eurocrypt 2005, pp. 491-506, 2005.

[4] J. Xiao and Z. Luo, "Multiterminal Source–Channel Communication Over an Orthogonal Multiple-Access Channel," Information Theory, IEEE Transactions on, vol. 53, pp. 3255-3264, 2007.

[5] P. Li, et al., "A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map," Physics Letters A, vol. 349, pp. 467-473, 2006.

[6] A. Canteaut, "Open problems related to algebraic attacks on stream ciphers," Coding and Cryptography, pp. 120-134, 2006.

[7] M. Mihaljevi , et al., "Cryptanalysis of keystream generator by decimated sample based algebraic and fast correlation attacks," Progress in Cryptology-INDOCRYPT 2005, pp. 155-168, 2005.

[8] W. Awad, "Finding Linear Equivalence of Key stream Generators Using Genetic Simulated Annealing," Information Technology Journal, vol. 7, pp. 541-544, 2008.

[9] K. Faraoun, "Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption," The International Arab Journal of Information Technology, vol. 7, pp. 231-239, 2010.

[10] R. Martin, et al., "Test-Driven Development," IEEE Software, vol. 24, pp. 32-36, 2007.